AD-A266 014

...CUMENTATION PAGE

Form Approved
OMB No. 0704-0188

2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
May 26, 1993	Final

4. TITLE AND SUBTITLE

Defense Information Infrastructure: Rationale for Defense Management Report Decision 918

5. FUNDING NUMBERS

6. AUTHOR(S)

Ms. Cynthia Kendall
Bill Beyer

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Same as 9 below

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

OASD (C31), DASD (IS)
The Pentagon, Rm 3E223
Washington, DC 20301

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

93-13163

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited.

93 6 11 058

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

On September 15, 1992, theDeputy Secretary of Defense approved Defense Management Report Decision 918, "Defense Information Infrastructure." The objective of this DMRD is to establish an information Infrastructure which provides a seamless, transparent, and protected end-to-end information transfer capability for DOD users. The paper "Defense Information Infrastructure: Rationale for Defense Management Report Decision 918, September 1992" provides the underlying assumption, principles and strategy which provided the basis for the concept of the approved DRMD. This paper describes the overall Defense Information Infrastructure (DII) and its role in support of joint operations. It defines those subelements of the Infrastructure for which the Defense Information Systems Agency (DISA) would have management responsibility (as envisioned in the development of the original DMRD), including a description of how DISA could operate and finance these functions. It outlines a potential sequence of actions to implement the information infrastructure that better supports our joint and combined forces. The paper may be useful to anyone who has an interest in the genesis of the DMRD, especially as a baseline document from which informed discussion of the DMRD may proceed.

14. SUBJECT TERMS	15. NUMBER OF PAGES
CIM (Corporate Information Management); DMRD 918; Defense Information Infrastructure (DII); Infrastructure; Defense Information Systems Agency (DISA)	29
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

C.I.M.

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-3040

COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE

MAY 26 1993

MEMORANDUM FOR DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARY OF DEFENSE (FORCE MANAGEMENT AND PERSONNEL)
ASSISTANT SECRETARY OF DEFENSE (HEALTH AFFAIRS)
ASSISTANT SECRETARY OF DEFENSE (PRODUCTION AND LOGISTICS)
ASSISTANT SECRETARY OF DEFENSE (PROGRAM ANALYSIS AND EVALUATION)
ASSISTANT SECRETARY OF DEFENSE (PUBLIC AFFAIRS)
ASSISTANT SECRETARY OF DEFENSE (RESERVE AFFAIRS)
COMPTROLLER
GENERAL COUNSEL
ASSISTANT SECRETARY OF THE NAVY (RESEARCH, DEVELOPMENT AND ACQUISITION)
DIRECTOR OF ADMINISTRATION AND MANAGEMENT
PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE (STRATEGY AND RESOURCES), OUSD (POLICY)
DIRECTOR OF INFORMATION SYSTEMS FOR COMMAND, CONTROL, COMMUNICATIONS AND COMPUTERS, ARMY
DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE (COMMUNICATIONS, COMPUTERS AND LOGISTICS)
DIRECTOR FOR COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS (J6), JOINT STAFF
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY

SUBJECT: Defense Management Report Decision (DMRD) 918 Reference Document

In a memorandum dated May 7, 1993, the Deputy Secretary of Defense expressed full commitment to the improvements, efficiencies and productivity gains of DMRD 918. However, pending further review and study, he placed planning and implementation actions on hold in procurement, communications and engineering (less the Defense Information Systems Network (DISN)), Central Design Activities, and Stage II. Other implementation activities such as Data Processing Installation consolidations, DISN consolidations, and Standards activities will be transferred as originally planned.

To assist in open deliberations on DMRD 918, attached for your information is a paper titled "Rationale for Defense Management Report Decision (DMRD) 918." This paper embodies the underlying rationale, concept of operations, strategy and philosophy used during the DMRD's development last summer. It is provided for your use as a reference only. It reflects eighteen months of benchmarking industry experience, modeling "information services utility" functions and other research which led to the development of the original DMRD approved on September 15, 1992.

It is the historical baseline or "start point" of the DMRD. Changes to this strategy have already occurred during development of the implementation plan and additional changes are likely to occur based on the May 7, 1993 memorandum. Copies of the "Rationale for Defense Management Report Decision (DMRD) 918" will be available from the Defense Technical Information Center by calling 1-800-CAL-DTIC in the mid-June timeframe.

The hard work and tireless effort of those involved with the planning for the implementation of DMRD 918 is appreciated. Of utmost importance is the patience and professionalism of those individuals currently under operational control of the Defense Information Systems Agency. Your continued support during this review period is very much appreciated.

C Kendall

Cynthia Kendall
Deputy Assistant Secretary of Defense
(Information Systems)

Attachment

DEFENSE

INFORMATION INFRASTRUCTURE:

RATIONALE

FOR

DEFENSE MANAGEMENT REPORT DECISION 918

September 1992

DEFENSE INFORMATION INFRASTRUCTURE

SEPTEMBER 1992

TABLE OF CONTENTS

I. FOREWORD

The Deputy Secretary of Defense approved Defense Management Report Decision (DMRD) 918, "Defense Information Infrastructure," on September 15, 1992. The objective of this DMRD is to establish an information infrastructure which provides a seamless, transparent, and protected end-to-end information transfer capability. This capability will: (1) revolutionize information exchange, defense-wide, (2) strengthen the DoD's ability to apply computing, communications, and information management capabilities to the accomplishment of the Department's mission, and (3) minimize information technology burdens on operational and functional staffs. Successful implementation will enable operational and functional staffs to access, share, and exchange information worldwide with minimal knowledge of communication and computing technologies.

This paper describes the overall Defense information infrastructure (DII) and its role in support of joint operations. It defines those sub-elements of the infrastructure for which the the Defense Information Systems Agency (DISA) would have management responsibility (as envisioned in the development of the original DMRD), including a description of how the DISA could operate and finance these functions. It outlines a potential sequence of actions to implement an information infrastructure that better supports our joint and combined forces.

This approach is based on best practices of world class organizations that have implemented similar capabilities. It has been adjusted to reflect the differences in the DoD, and to take advantage of ongoing information technology management initiatives.

II. THE CONCEPT

Automation, advanced electronics, worldwide communications, and modern sensors provide a quantum improvement in the efficiency with which force can be applied on the battlefield. Application of these technologies has vastly increased the amount of information needed to run any military operation, and made information management pivotal to managing the employment of military force. In modern war, the flow of information from our support functions is so essential that it must be integrated into the same information domain as the command, control, computing, communications, and intelligence (C4I) functions. C4I assets can no longer be viewed as separate programs and systems that are partitioned along the historical lines of strategic command and control, tactical command and control, defense-wide systems, intelligence, and business. Interoperability between command and control, intelligence, and business systems has become a mandatory requirement.

Although the DoD emphasizes technological sophistication, and spends over $20 billion each year on information technology, there is a persistent inability to protect, exchange, and combine critical information among command and control, intelligence, combat support, simulation and training, and business systems. The solution to these deficiencies is for the DoD to establish an information infrastructure[1] which is capable of supporting collection, generation, storage, display, and dissemination of information, Department-wide. The infrastructure should encompass end-to-end communications from wide area to local base level, tactical, and strategic connectivity; and data processing services for regional, local, and tactical requirements. It should support all military activities, whether in garrison during peacetime, mobilized in rapid deployment, or deployed in sustained war operations. The fixed, primary infrastructure should include the following elements:

(1) Long-haul and local communications backbone with networking and routing based on information content and management (determined by the user).

(2) Communications gateways for extensions beyond the primary infrastructure (e.g., to theater and tactical forces).

(3) Automated processing accessible to remote users through the communications network.

(4) Consolidated C4I support with integrated common-user functional areas (e.g., intelligence processing, meteorology, wide-area surveillance processing).

---

1 The Defense information infrastructure is defined as the worldwide aggregation of all mobile and fixed DoD information systems, including sensors, data entry devices, communication networks, computer resources, facilities, and operational and support staff which are organized to provide protection, collection, generation, storage, display, and dissemination of information to the DoD.

(5) Facilities to support commanders and staffs at echelons above the tactical commands and to host consolidated C4I support centers.

(6) A well-defined set of functions, information, and processing that is easily accessible by deployed forces in any theater or region. It should allow rapid, efficient flow of information from national or regional sources directly to the warfighters as they need it.

(7) A regional orientation toward capabilities that are most important for each area of operations with an inherent ability to focus additional national resources into the region as needed.

Under this concept, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) envisions an information infrastructure that is transparent to its users, improves reliability and service at lower costs, facilitates full implementation of corporate information management[2] principles, and responds to national security and defense needs in an efficient and effective manner. To achieve seamless, transparent support down to a mobile tactical element, deployed assets will be light in weight, small in cube, and able to interconnect with the primary infrastructure from anywhere in the world, i.e., a "plug and play" C4I structure. Information will flow smoothly without having to first solve compatibility and interoperability problems. (Figures 1 and 2 depict this information flow from a geographic and joint task force commander's perspectives, respectively.) Fixed and mobile C4I structures will be configured to move information without regard to organization or Service boundaries. The DoD will be able to focus on the information which it must generate, store, move, and protect. Further, as the vital resource of modern warfare, information will be protected commensurate with its intended use. Information systems will be choice targets, and we will need to minimize their vulnerability to hostile action.

Implementation of a C4 architecture that supports joint and combined operations will be done in stages which build on today's computing and communications foundation. The DoD will progressively integrate technologies and applications, worldwide, with emphasis on central management to achieve balanced solutions. An integrated, centrally managed infrastructure is the means to lessen information processing and transmission costs, reduce the number of information technology (IT) personnel, and streamline delivery time for IT products and services. Ultimately, the DoD's warfighting capability will improve through the increased availability of information that is needed to defeat adversaries. The right information will be available when and where it can be applied with success. Further, information will be "pulled" as needed, not just "pushed" out to overload recipients. Accomplishment of this goal will allow the Department to retain a decisive military advantage even as we reduce dramatically in size.

---

2 Corporate information management (CIM) is the Department's program to streamline its business, command and control, and intelligence processes, and evolve to standard applications systems. Key elements of CIM are standard business process re-engineering using the Integrated Definition tool; functional economic analysis techniques; data element and data management standardization programs; development of data, application, and infrastructure technical architectures; an application code repository program; and an Integrated Computer Assisted Software Engineering specification and acquisition program.

INFORMATION FLOW TO THE COMBATANT

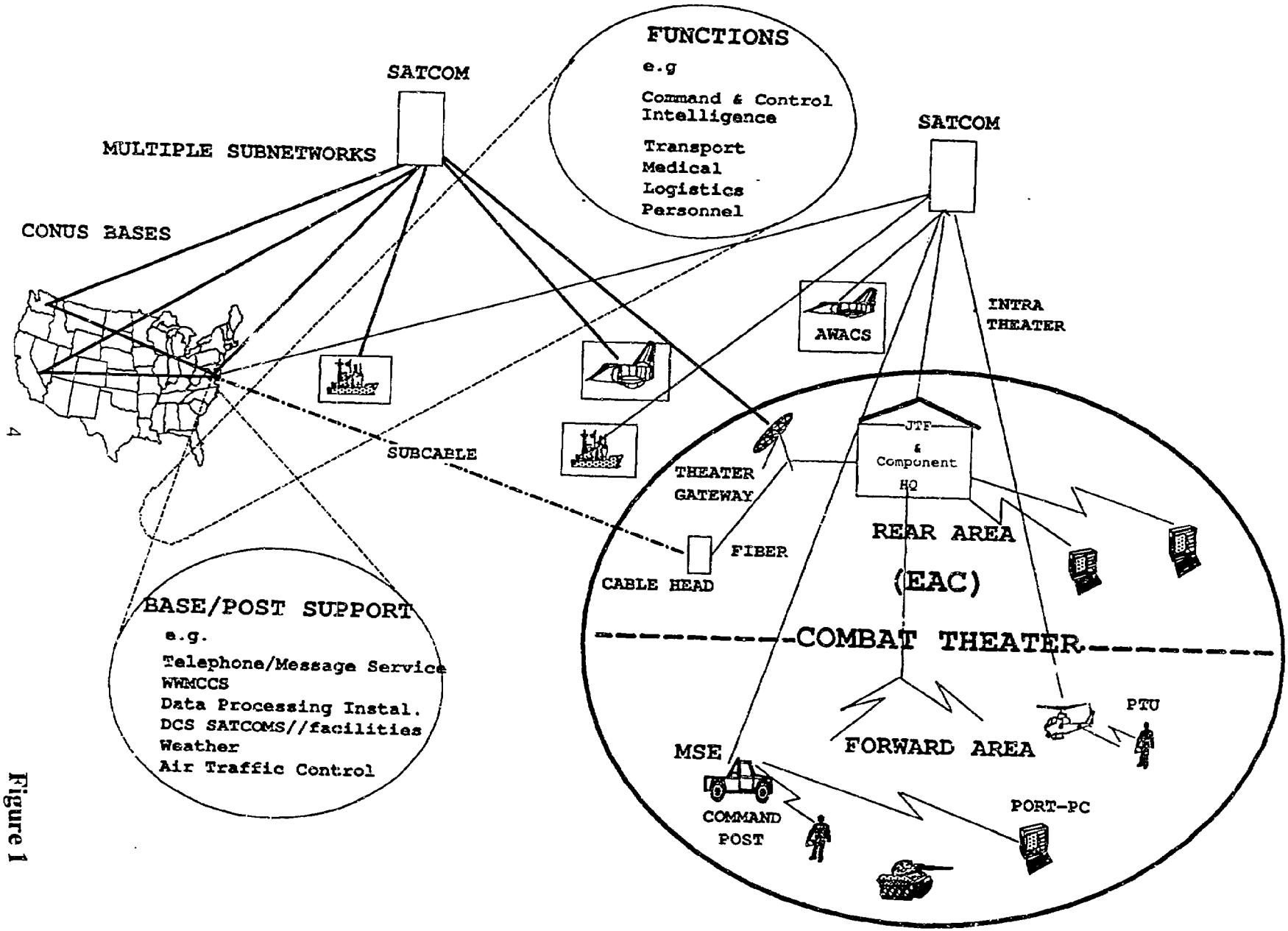

Figure 1

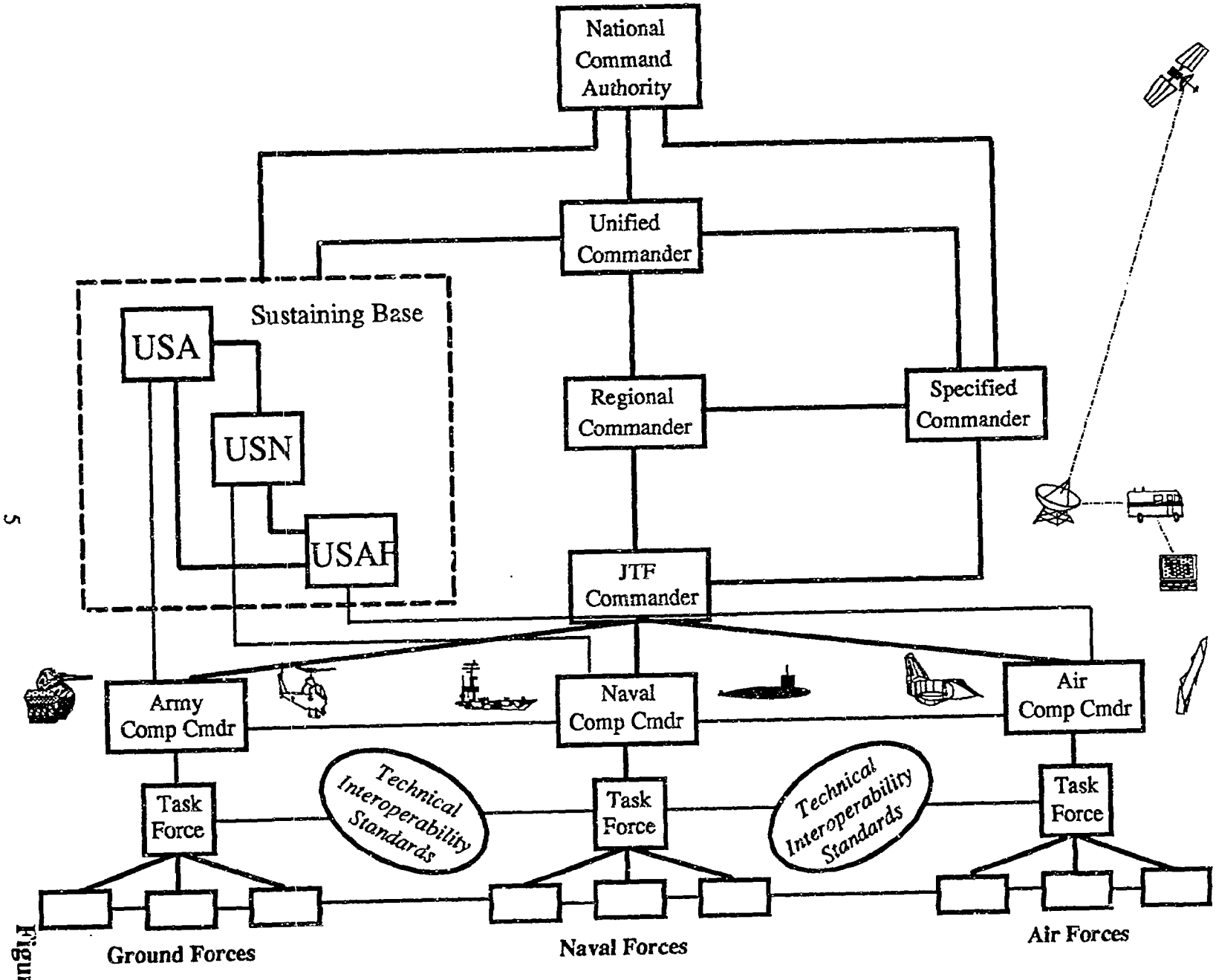
National Command Authority
Unified Commander
Sustaining Base
USA
USN
USAF
Regional Commander
Specified Commander
JTF Commander
Army Comp Cmdr
Naval Comp Cmdr
Air Comp Cmdr
Task Force
Task Force
Task Force
Technical Interoperability Standards
Technical Interoperability Standards
Ground Forces
Naval Forces
Air Forces

Figure 2

III. DEFENSE INFORMATION INFRASTRUCTURE OPERATIONS

The DISA, as central manager of the Defense information infrastructure, will manage the DoD communications support networks requiring systems integration (e.g., interfaces with defense communication systems) including local access switches, network control centers, central data processing operations, and software development for all applications managed under the corporate information management initiative. The DISA's responsibilities will encompass: (1) application of information systems security, (2) development, specification, certification, and enforcement of IT standards, (3) network management, engineering, design, and control of long haul, regional communications, and base level communications, (4) operation of long haul networks, (5) management and operations of DPIs and CDAs for support systems activities, (6) acquisition of IT components and services that require integration. Figure 3 provides additional detail on the scope of the DISA's responsibilities.

The following areas are excluded from the DISA's resource management: (1) command, control and communication systems that are integrally designed into weapon systems, are unique to and usually delivered with, or as part of an aircraft, missile complex, ship, van, etc., the costs of which normally are included in the cost of weapon systems; (2) IT resources dedicated to support strategic and tactical command, control, and intelligence missions, and wargaming. Although these categories are excluded for resource management purposes, they remain subject to the DISA's IT standards. In addition, local operations of computing (to include local switches, applications servers, local area networks and distributed office automation systems) may remain with Defense Components, subject to local option. The DISA will have authority to direct and control the technical specifications of these assets consistent with their technology management of the information infrastructure. Also, the Defense Components may serve local commanders' ad hoc needs for unique queries and reports. The Components will not have authority to create any new data elements for transmission into the local gateway or to make any modifications to corporate information management applications which would encumber the DISA's overall configuration management and control.

This approach invests the DISA with the central control and authority to implement a homogeneous, protected, quality defense information infrastructure. Operational and functional staffs will have a single DISA technical point of contact that can obtain for them the skills and corporate knowledge required to resolve complex computing and communication problems. This "one stop shopping" approach will reduce significantly the IT burdens on functional staffs, and enable them to access, share, and exchange information worldwide with minimal knowledge of communication and computing technologies. This approach will improve coordination and management across disciplines, and take full advantage of economies of scale where consolidation of functions can satisfy requirements for IT goods and services.

RESPONSIBILITY FOR THE FUNCTION COMES TO, OR STAYS IN DISA (YES OR NO)

		OWN	OPERATE AND MAINT.	PEO AND PM	PROCURE	MANAGE CONNECTIVITY OR CAPACITY	TECH. OVER-SIGHT	ENGI-NIEERING	INSTAL-LATION	SEC-URITY	STAN-DARDS	CONFIG. MGMT.
Long Haul	- DCS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	- DCSC	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Gateway	e.g., DCO, Comm Ctr, SAT GND entry	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Base Level	- Base Comm	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
	- LANs	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
	- Base Computing (Non-DPI)	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
	- Office Automation	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
DPIs		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CDAs		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Figure 3

The DISA will be the focal point within the Department for the following capabilities:

1. IT equipment and software acquisition (reuse, recondition, new system acquisition - lease or buy).

2. Information processing, system design, analysis, and programming services, and systems integration.

3. Communication services to include adaptive central network management and control, network design, engineering, and systems integration.

4. On-line directories of DoD organizations and personnel.

5. Integrated Computer Assisted Software Engineering tool set for systems developers.

6. Central knowledge repository to support business process improvement to include:

   a. Key business process, data, and activity cost models;

   b. Information about IT systems (both IT equipment and applications with resources linked to the Planning, Programming, Budget, and Execution System and business processes);

   c. Information about IT suppliers and their products;

   d. Directory of other on-line databases;

   e. Applicable standards and specifications;

   f. Best industry and government business practices;

   g. Standard cost information to assist functional economic analysis development; and

   h. On-line catalog of the DISA services.

Customer business units (CBUs) within the DISA will serve as the primary point of contact for customers; key among these are the Principal Staff Assistants (PSAs)[3]. Figure 4 depicts this relationship. Each CBU will have customers -- PSAs, DoD Components, and commanders-in-chief of the unified and specified commands -- for which it is dedicated to providing IT services and products under a service level agreement. The DISA will assess and report performance and customer satisfaction against these negotiated agreements. The DISA will broker incoming IT work to the most capable, high performing suppliers; thereby, allowing customers to move to sources that can supply services most effectively, and at the lowest cost.

---

3 To ensure accountability, the PSAs will have input into the CBU performance appraisals.

The suppliers will include DoD IT activities (e.g., data processing installations, central design activities, etc.), other government agencies, and commercial vendors.

A typical transaction will involve a customer developing a functional economic analysis for a requirement using the DISA's supplier catalogues and business process model repositories. Once the requirement is approved by the appropriate PSA and funded, it will be provided to the CBU for engineering of alternative technical solutions. Alternatives will be negotiated with the customer, and agreements documented in a service level agreement. Products and services will be delivered in accordance with the terms of the agreements or the provider will incur performance penalties for those periods when the level of services does not meet stipulated standards. Figures 5 and 6 provide examples of the interplay amongst various functions within the DISA when supporting a customer and an infrastructure requirement.

CONCEPT OF OPERATIONS

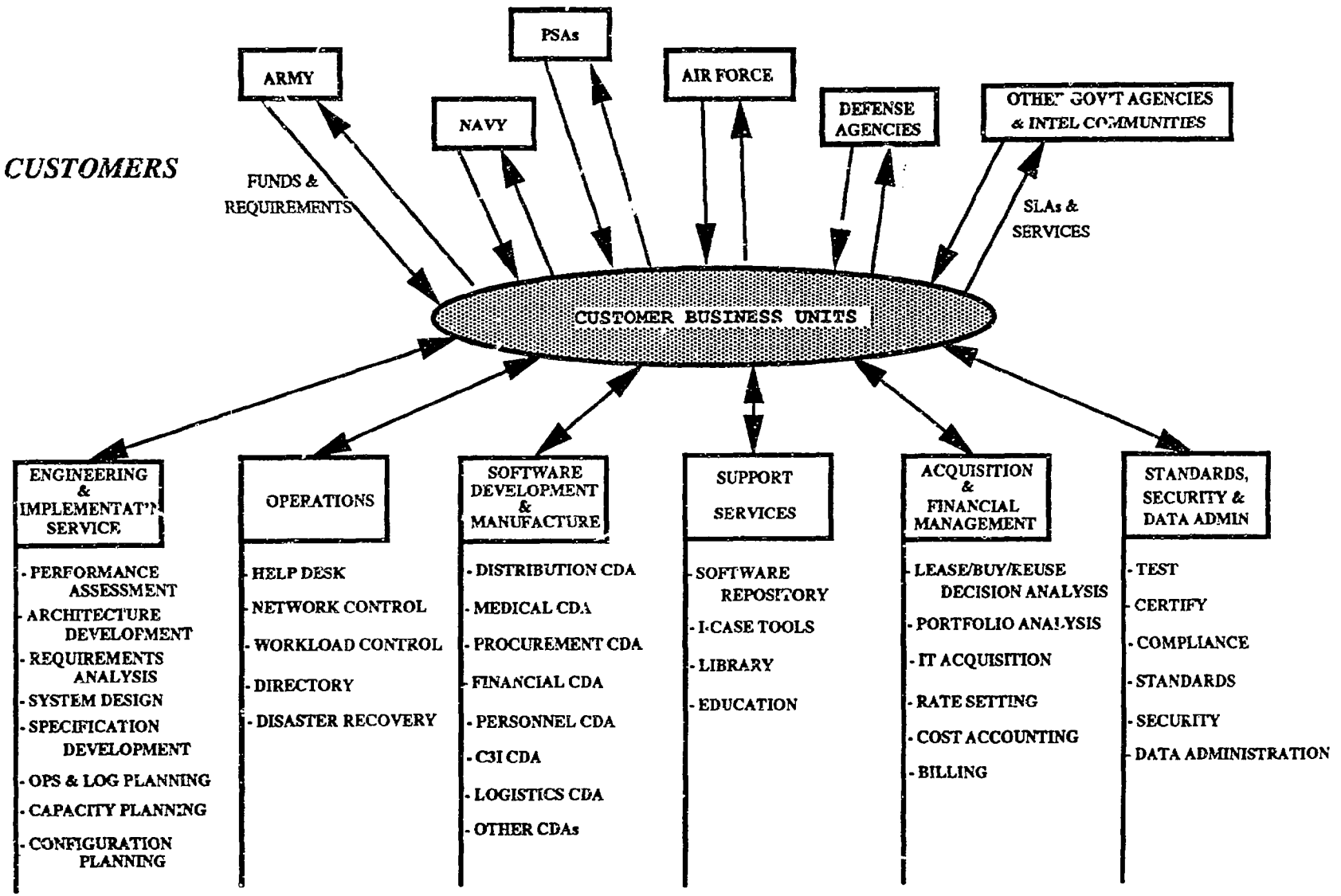

Figure 4

Customer Requirement for Development or Modernization

Figure 5

Modernizing the Infrastructure: A Technology Upgrade

Figure 6

IV. IMPLEMENTATION STRATEGIES

There are a number of private sector companies that are similar to the Department in that they are highly complex organizations with a multinational presence, deploying large numbers of personnel and considerable resources. Also like the Department, many of these companies were faced with slow death from fractionated and incomplete development, operation, and support of their communications, computing, and information management services. Many of them would not be in business today if they had not consolidated and centralized their IT resources.

The lessons learned from these companies, with their many similarities to the DoD, form the basis for the implementation strategy presented in this chapter. Thus, the strategy is based on actual practices, not merely theory. These practices were analyzed to determine what worked best for industry. Then, they were adapted to adjust for unique DoD requirements such as secure interoperability, the sheer size and complexity of operations, ongoing IT management initiatives, and legislation. Implementation in a government environment presents special challenges. These challenges required some modification to the strategy, but enough similarities existed to avoid wholesale revision or substitution. Examples of specific adjustments include exclusion of command, control, intelligence, and tactical communications areas for centralization; slowing the pace of implementation; and allowing considerable additional time to reach the break-even point by lowering the rate of savings and increasing the level of investments.

Companies which established world class information management organizations went through a standard process[4]. There are two parts to this process. First, management establishes control over the information infrastructure, to include how it is managed and used. Second, the effectiveness and efficiency of the infrastructure is improved. Within these parts, the sequencing of steps are critical to the successful development of a fully integrated computing and communications infrastructure. These steps are portrayed in Figure 7. The remainder of this chapter presents a description of these steps.

A. Management Control - Part 1

As the first step in an undertaking of this magnitude, comprehensive planning activities must occur at all levels. All activities taken together must answer the questions -- Are we doing the right thing, and are we doing things right? Planning activities must concentrate on the customer, and include an analysis of future demands for information infrastructure services. This business process analysis must precede any discussions about information technology

---

4 These companies were identified in discussions with ADAPSO, CAM-I, and over 50 of the top information management organizations of the world. They include companies such as EDS, Boeing, General Dynamics, GTE, CSC, CITICORP, and the Harris Corporation.

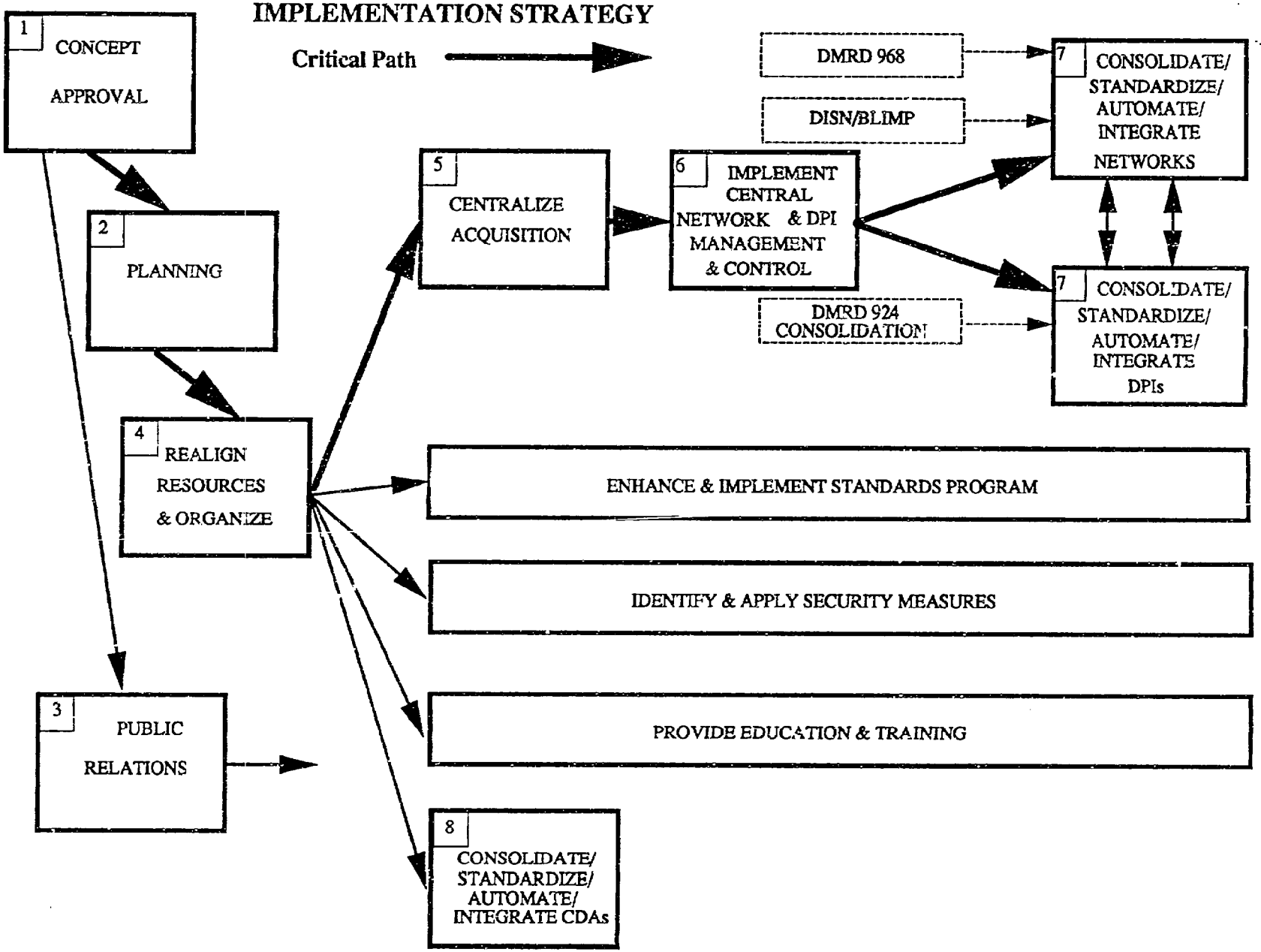
IMPLEMENTATION STRATEGY
Critical Path
1 CONCEPT APPROVAL
2 PLANNING
3 PUBLIC RELATIONS
4 REALIGN RESOURCES & ORGANIZE
5 CENTRALIZE ACQUISITION
6 IMPLEMENT CENTRAL NETWORK & DPI MANAGEMENT & CONTROL
DMRD 968
DISN/BLIMP
DMRD 924 CONSOLIDATION
7 CONSOLIDATE/ STANDARDIZE/ AUTOMATE/ INTEGRATE NETWORKS
7 CONSOLIDATE/ STANDARDIZE/ AUTOMATE/ INTEGRATE DPIs
ENHANCE & IMPLEMENT STANDARDS PROGRAM
IDENTIFY & APPLY SECURITY MEASURES
PROVIDE EDUCATION & TRAINING
8 CONSOLIDATE/ STANDARDIZE/ AUTOMATE/ INTEGRATE CDAs

Figure 7

strategies. The uncompromising analysis and discussion of what the customer needs and how the proposed activities will satisfy them, at every stage of development, should be an essential characteristic of these planning activities.

Well-defined implementation procedures and processes, based on strategic planning and measurable quality objectives, must be in place before beginning to apply technical solutions. Extensive planning and analysis has been completed over the past twenty four months, and the DISA should build upon these earlier efforts (e.g., the Defense Information System Network strategic plan, the Command and Control Functional Analysis and Consolidation Review Panel Report, and the Joint Chiefs of Staff "C4I for the Warrior" concept).

A strong management and technical team is also essential. In addition to planning and implementation responsibilities, this team should be given the responsibility for ensuring the implementation plan and its goals are disseminated, understood, and supported by all levels within the Department. This information infrastructure concept is a radical departure from the traditional approaches taken for the collection, generation, storage, display and dissemination of information within DoD. A massive effort, using all media with a wide dissemination, is required to make people within the DoD and industry aware of these changes and their advantages.

After initial planning, the DISA should establish basic control mechanisms to successfully function as central manager of the Defense information infrastructure. These controls are crucial to the DISA's implementation of a protected end-to-end information transfer capability. Industry experience shows that the technologist (i.e., the DISA) must completely control the construction of an integrated information infrastructure. The functional manager pays the cost, and the technologist routinely demonstrates, through fee-for-service and quantifiable performance measures, that the infrastructure is efficiently meeting IT needs. These controls permit the DISA to build in safeguards to minimize risk to implementation; ensure the transition is transparent to users who are assured uninterrupted services and interoperability; minimize personnel turbulence; and create an environment where resources, equipment, and people can be best managed and leveraged. Successful companies accomplished the first stage in this order:

1. Realign resources immediately

❒ Immediately realign IT personnel to establish an organization to centrally manage and construct the Defense information infrastructure. This causes less turmoil by realigning personnel only once; thereby, allowing people to know promptly where they stand. It exposes unnecessary duplication. Also, it permits a synergistic mix of critical skills that contributes to the efficient and effective management of resources. It also stops IT activity outside of management control.

❒ Provide three to five days of indoctrination into the DISA mission and organization for personnel realigned to the DISA. These training sessions should focus on how the changes affect the people, why change is needed, when key events will occur, and how they can effectively contribute to the change. Establish performance measurement criteria which include a reward and appraisal system that will encourage teamwork among personnel assigned to the DISA, and emphasize employee empowerment at the DISA. Tie

performance incentives to the performance of the infrastructure to ensure responsive and economical operations.

2. Centralize acquisition of information technology equipment and services

❒ Centralize acquisition activities before taking steps to consolidate, standardize, automate, or integrate the communications networks and data processing installations (DPI). This ensures efficient and effective acquisition of IT equipment and software to implement an integrated infrastructure. Specifically, it reduces procurement leadtime, allows for the rapid infusion of new technologies, maximizes investments, and prevents unauthorized acquisitions of duplicative, nonstandard, disparate IT equipment and software.

❒ Establish market research and portfolio analysis capabilities consisting of a dedicated team of financial analysts, engineers, and procurement specialists who stay constantly in tune with the customers and the market place to assess and match customer needs with both the available technology, and the most economical methods of acquiring this technology based on functional economic analyses. Conduct ongoing technical and financial evaluations of the market place. Continually test and evaluate current products. Analyze the equipment and software markets and make recommendations, based on product life cycle analysis, to buy or lease new hardware and software release. Revisit lease and buy decisions on a monthly basis. Ensure that the infrastructure portfolio investments are producing savings and assess the impact of changes on previous savings decisions.

❒ Influence IT products from industry. A centralized IT acquisition function enhances the Department's ability to leverage industry by resulting in larger acquisitions which emphasize the importance of DoD as a customer, and maximizes the use of standard procurement specifications. Where possible, use commercial off-the-shelf and nondevelopment item products. This ensures the DoD moves rapidly towards open systems, and allows for software compliance. Clear standards profiles are essential.

❒ Provide immediate savings through economic quantity orders and reduced contract overhead which are realigned to provide investments in central network management and control and DPI management and workload control.

3. Centralize network management and control while concurrently centralizing DPI management and workload control

❒ Ensure network management and control systems are in place, operational, and integrated to enable the DISA to effectively manage end-to-end (i.e., keyboard to keyboard) information transfer services. Otherwise, industry experience shows that other implementation activities such as circuit bundling quickly outpace network operations and support systems deployment, and suboptimize efforts to consolidate, standardize, automate, and integrate. Establish new, improved methods for real-time network management to manage the operation of a network of this size and complexity. Advanced automation is essential to implement real-time control systems. Real-time network

management will provide substantial cost reductions, both by using existing network resources more effectively, and by reducing the current manpower intensive aspects of network management. Such capabilities are important not only for optimum operation, but are also essential to permit the highly complex network to respond quickly to requests for reconfiguration, or to recover from damage or destruction. Develop a strategy related to DPI workload distribution to maximize economies of scale in the processing of information. Operational efficiency is enhanced by bringing similar and common applications into the same, larger DPI. Physically collocate network control and DPI workload control. EDS and GTE are examples of companies that collocated these functions.

❒ Establish an integrated central management capability to include:

a. Technical architecture development and procedures for keeping it current.

b. Procedures for managing change in five areas -- technical, time, user requirements, geographic, and regulatory/tariff.

c. Performance management - performance data collection, performance monitoring, traffic management, quality assurance, and network design.

d. Fault management - alarm surveillance, failure localization, trouble desk, quality assurance tests, backup procedures, and corrective maintenance.

e. Configuration management - service provisioning, status and control, and installation.

f. Accounting management - collection of usage data.

g. Security management - user authentication, protection from software intrusions, access control, key management, and audit trails.

h. Procedures for dynamic rerouting of workload.

i. Remote monitoring of workload.

j. Help desk.

B. Improving the effectiveness and efficiency of the infrastructure - Part II

Once the above controls are established under the first stage, the DISA can focus on steps to achieve steady cost reductions, and generate savings (a portion of which can be realigned to support investments in modernizing the infrastructure). Successful companies accomplished the second stage in this order:

1. Consolidate networks and DPIs

❒ Consolidate the infrastructure to provide fewer communication problems, less duplicative effort and overhead, and more efficient use of resources, hardware, and people. This is the first step towards maximum efficiency in the use of DoD's communications and computing resources. This step involves consolidation of over 100 independent, long haul DoD networks into a single common-user transmission network. Consolidate individual circuits into a T-1/T-3 network for DoD-wide use and capitalize on the DoD Components' dedicated circuit bundling efforts. For DPIs, this step reduces or eliminates the mainframe and minicomputer sites ignored under DMRD 924, and migrates the 43 centers created under DMRD 924 to 10 - 30 DoD megacenters. Configure each megacenter to provide at least 600 MIPS of capacity. Address capacity planning issues early in the planning process. Quantify and evaluate the basic workload currently being processed, the forecasted future workload, the forecast of new application systems, and any other changes foreseen. Consolidation leads to standardization of the operating environment. Examples of the criteria that might be used to select megacenters are:

a. Protected and certified to have superior security and backup power.

b. Education and training capability.

c. Superior quality of life.

d. Seasoned, top caliber personnel.

e. On garrison (physical security).

f. Existing site.

g. Expandable to 100,000 sq. ft..

h. Dual independent power supply source.

i. Backup and disaster recovery capability.

j. On Level I and II fiber optics.

2. Standardize networks and DPIs

❒ Make maximum use of standardized practices, procedures, and procurement specifications, once the infrastructure is consolidated. Reduced administrative costs, reduced implementation time frames, and uniform network and DPI technical capabilities are the benefits of this step. Also, adhere to current and future national and international standards to facilitate enterprisewide processing, interconnection, and communication.

3. Automate networks and DPIs

❒ Automate organizational support systems such as service order processing, complaint management and follow-up, billing, equipment and circuit inventory, business analysis planning, performance trending, cost management, and plant optimization. Achieve efficiencies through the introduction of automation in the DPI environment to include "lights out" operations, console automation systems, cassette library management, job scheduling systems, and job balancing systems.

4. Integrate networks and DPIs

❒ Eliminate real demarcations (where technical solutions are lashed up) between networks and processing to provide the end-to-end connectivity necessary to support the transmission and reception of information through an ubiquitous global network. Increasing distribution of computer power (by the year 2000, 95% of MIPS will have migrated to desktops and megacenters will host the data servers) creates a design need for networks that are highly meshed, providing user-to-user connectivity. Practically speaking, there is only one network, and LAN, MAN, WAN subnets (both logical and physical) are all part of the same network, an enterprise network.

C. Information Security, Standards, and Education and Training

Information security, standards, and education and training are essential to the completeness of the Defense information infrastructure. These three elements should be viewed as an integral part of the above steps (e.g., security must be designed into networks and DPIs), rather than as separate and distinct entities onto themselves.

1. Information security

This is a major area where Defense requirements exceed those of industry. Increases in the amount of information and data, as well as in the numbers and configurations of communications and computer systems, provide increased accessibility, expanded opportunities for exploitation, and proportional increases in potential benefits to the exploiter. The level of sophistication of attacks will steadily improve against both communications and computer systems. Network and computer systems are vulnerable to internal as well as external threats, including viruses and other sophisticated techniques. Those seeking to exploit information systems, which include not only external threats such as hackers and other unauthorized users, but internal "authorized" sources as well, pose a formidable challenge. These adversaries have become not only more sophisticated in their methods of exploitation, but also more aggressive in their attempts to steal, manipulate, and destroy data.

Therefore, specific actions for security improvement by the DISA must include: (1) establishing a top-down determination of which information needs protection and the extent of protection needed as part of the overall architecture, (2) improving management oversight, review, execution, and cross-discipline analysis of counterintelligence and security countermeasures, especially as a part of the network management step, (3) establishing mechanisms to ensure appropriate information security policies are implemented as part of all corporate

information management architectures, networks, and systems, and (4) improving security and counterintelligence awareness and training among DoD functional managers and supervisors. Security should be considered during design and acquisition, and policed through network control. The DISA should develop a program which addresses:

❒ Security policy analysis. Define, coordinate, and recommend a comprehensive and coherent information systems security policy for defense information systems that is consistent with national level policies.

❒ Security architecture. Define, coordinate, issue, and maintain defense information systems security architectures based on a comprehensive assessment of threat, vulnerability, and risk faced by information systems together with a cost and performance analyses of systems alternatives.

❒ Security standards and protocols. Review, coordinate, and recommend information systems security standards and protocols for effective interconnection of information systems in accordance with the defense information systems security architecture. Accelerate development of security standards which will promote security integration, interoperability, and data sharing among systems.

❒ Security evaluation, certification, and accreditation procedures. Review, coordinate, and recommend security evaluation, certification, and accreditation procedures for defense information systems. Assess security certification and accreditation standards, guidelines and directives, and propose revisions as needed.

❒ Security technology. Define information security technology to instantiate the defense information systems security architecture, and identify resources necessary to provide this technology. This includes identification of common security requirements that may require government-unique development of security products.

❒ Transition plan. Define, coordinate, and maintain a master transition plan to take DoD to full implementation of the defense information systems security architecture.

❒ Coordination and cooperation. Improve coordination and cooperation among organizations developing, implementing, and operating defense automated information systems and networks.

❒ Security products and security focus. Provide a focused and coherent view of defense information systems security needs to vendors of information systems products and services.

2. IT standards

The thrust of this effort is to accelerate the transition to commercial and Federal Information Processing Standards. The DISA's Center for Standards serves as the mechanism for adopting, developing, specifying, certifying and enforcing standards, DoD-wide, and it must work closely with the DISA's acquisition function. The categories - command, control and communications systems that are integrally designed into weapon systems; IT resources dedicated

to strategic and tactical command, control, and intelligence missions; and wargaming - are subject to information technology standards. The Center must develop:

- ❒ A consistent set of community and domain specific standards profiles.
- ❒ Standards and standards profile support. This will include standards reference documents, standards guidance documents, and assistance in profile development.
- ❒ A standards activity coordination process.
- ❒ A standards issue resolution process.
- ❒ The capability to enforce standards. Standards, without an enforcement process, are not sufficient to achieve a world class, protected, seamless, and transparent information infrastructure as documented in lessons learned by the Joint Staff and industry. To enforce standards, the DISA must have control of acquisition, network and configura[illegible] control, and overall architecture and design integrity.

In addition, the Center must coordinate profiles across the DoD, certify profiles, identify standards needs, and ensure appropriate standards are available.

3. Education and training

New skills, innovative career development, and state-of-the-art education and training (in terms of both content and development) are key to bringing about the improvements in human performance needed to support implementation of the IT components described above. Career development must weave in leadership, business management, and customer focus education as well as technical skills training. Education and training are essential to ensuring that people can perform well, that they can work together effectively, and that their skills are state of the art. Implementation of these goals will provide the DoD with a technically rich, professionally diverse information systems workforce for the 21st century. The ASD(C3I) will establish an executive agent to (1) develop specific education and training standards, curriculum, and delivery systems, and (2) develop civilian IT career paths and certification standards and programs. The agent will manage all IT education and training organizations. The executive agent will oversee the execution of the IT education and career path/certification programs. Responsibilities include:

- ❒ Develop a comprehensive DoD-wide IT technical and managerial education and training plan;
- ❒ Ensure a coordinated IT technical and managerial curriculum is available to DoD users;
- ❒ Oversee development of needed IT courses;
- ❒ Deliver or manage the delivery of associated education and training:

❒ Serve as the IT technical and managerial education and training "clearinghouse" for the Department;

❒ Develop an IRM certification program; and

❒ Ensure training exercises adequately stress communications and computing systems and personnel, and that IT education and training shortfalls are incorporated into future courses.

D. Central Design Activities

Implementation of the above steps will result in a fully integrated, protected enterprise level computing and communications infrastructure. In addition, the DISA must address system development resources at central design activities (CDA) to leverage technical and application area expertise in support of the DoD's business activities. Although CDAs are not on the critical path for establishing the integrated computing and communications infrastructure, they are a key element for achieving savings and improving the quality of applications. Industry began the consolidation of applications after the physical infrastructure was in place. Companies are now in the database creation stage, the first step to a distributed architecture. With DMRD 925, the DoD has already begun the standardization of applications.

Functional proponents are responsible for determining information requirements, while the DISA manages and operates the CDAs to ensure they effectively accommodate these requirements. Industry experience shows that consolidation of CDAs results in significant improvements in efficiency, effectiveness, and quality. Consolidation of application development resources is pursued concurrent with steps to implement the computing and communications infrastructure. Initially, decisions are made relative to the structure of CDAs and system integration activities organization. Centers of expertise are formed around critical application system development skills as a resource for all of DoD. Some of these centers focus on specific business areas and multi-business areas, others on particular technology as applied to business areas, and still others on key development support skills, e.g., CASE tool assessment. This approach helps significantly in managing emerging technologies by providing a focal point for the DISA, and enabling the building of critical mass of scarce expertise in emerging fields.

1. Organize CDA resources

❒ Develop a master CDA plan in conjunction with the Principal Staff Assistants (PSAs) to carefully structure consolidated CDA organizations to ensure that they effectively serve the DoD's needs. Identify the balance between the various organizational considerations (function, business area, geography, emerging technology, centers of expertise) that provides the best mix to optimize the management of CDAs.

2. Consolidate CDAs

❒ Stage CDA consolidations incrementally to ensure continuity of operations. Consolidate several of the largest CDAs first. They provide the best opportunities for eliminating

redundancy and improving effectiveness. In addition, this provides some important learning, and sets the stage for subsequent consolidations.

3. Standardize CDAs

❒ Work with the PSAs through the corporate information management process to focus CDA efforts on system integration and standard software applications. Having people who are working on similar systems for different customers in the same environment helps drive toward commonization.

4. Automate CDAs

❒ Improve the quality of applications by implementing automated tools such as an Integrated Computer Assisted Software Engineering tool set. Industry has shown a factor-of-ten improvement in software reliability and maintainability using such tools. This is essential for achieving massive reductions in software costs. Establish widespread networking of workstations so that several system analysts can work together on different components of a large project. Establish an on-line library of reusable code, designs, and specifications.

5. Integrate CDAs

❒ Work with the PSAs to migrate functional CDAs towards business areas on the basis of a DoD enterprise architecture. CDA support should be by business area with the CDAs' responsible for systems integration.

V. FINANCING STRATEGIES

The DISA information infrastructure will operate on a fee-for-service basis under the Information Services business area of the Defense Business Operations Fund (DBOF). Customers retain funding for IT services and products within their budgets. They establish requirements, and are charged by the DISA on a legible monthly basis (i.e., like a phone bill) for the cost of services and products, provided through the DISA's stabilized rate structure. The bill covers all charges to include infrastructure investments, which will be depreciated, and overhead. The DISA incurs costs based on infrastructure needs to support customer orders. The DISA is responsible for producing quality IT products and services which satisfy customer requirements at the lowest cost.

Fee-for-service is a vitally important concept for several reasons. It establishes accountability for both customers and the DISA. With fee-for-service, the customer, whose program the DISA supports, is responsible and accountable for the products of that support. When customers are accountable for IT costs, they can make value judgments regarding the use of these services. If IT services are provided at zero cost to customers, infinite resources are consumed, and noncritical requirements have the same priorities as critical requirements. If the DISA must earn revenue for service, the DISA has to monitor their costs closely. Costs will be carefully scrutinized by customers. It is the DISA's responsibility to broker work to the most capable, high performing suppliers. Those suppliers who do not operate efficiently will lose customers, and face decreasing levels of business activity. This linkage between IT costs to customer funding ensures continuous communication between the customer and the DISA. Additionally, the DISA managers can identify cost drivers, and focus their management improvement efforts accordingly.

Direct funding remains in the customer budgets, and customers justify IT workload and expenditures, as part of their business operations, through their normal budget process. The DISA consolidates approved workloads, and determines the information resources needed to supply the projected capability. The DISA will set and justify rates based on the capacity needed to support projected workload and traffic. The focus of the DISA's justification is to ensure that the estimate for total information resources is appropriate. This places the burden of justifying IT expenditures on the customers, and the burden of satisfying the cost of those requirements on the DISA.

Through fee-for-service and the DBOF, the DISA achieves a business relationship with its customers. The fund expands the availability of business management information, and provides a structure that supports the customer-provider relationship. This business management structure encourages the DISA managers and employees to provide quality IT products and services at the lowest cost. Otherwise, the DISA may not be responsive to customer needs. Managing to total cost provides increased flexibility to both DISA customers and the DISA itself. Customers have the visibility of the true costs of their IT requirements, so that effective trade-off decisions can be made between information processing costs and their business value. The DISA, on the other hand, has visibility of its total costs in satisfying customer requirements

so that processes used in producing IT products or providing IT services can be evaluated, and continuous productivity improvements and efficiencies implemented. In addition, the DISA improves its capacity management through alternative pricing options (e.g., peak load pricing, response time options, etc.) to influence customer behavior.

Under the concept of operations, the DISA provides an immense range of services on an unparalleled scale. There has never been an IT organization in the Department that has provided a comparable array of services on a fee-for-service basis. Although this greatly increases the complexity of the rate structure, rates must be established quickly, and their price must be based on an accurate relation of activities to products and services. Rates must be based on outputs which are in understandable workload units. This is imperative to encourage smart decision making by customers. Customers cannot become accountable if they have to translate IT costs into the management information for which they receive value. Through rates, customers are: (1) made aware of the full cost of IT services provided to them, (2) made responsible for the cost of the services they use, and (3) motivated to make decisions about the use of IT services on the basis of their cost. Rates become a performance incentive for customers and the DISA. Incorrect pricing results in poor decisions that could be disastrous for the Department; thus, the DISA regulatory board (Rate Management Council) that oversees these rates must include customer representatives.

The DBOF provides the framework for evaluating DISA investment requirements in terms of operational cost. For example, if a DISA manager determines that an investment helps achieve long-term lower costs, there is more of an incentive to make that investment. All IT capital investments are included in a capital budget and depreciated. The depreciation costs then become part of the DISA rate structure to provide an IT product or service. Benefits are realized from IT capital investments, either through efficiencies or reduced costs. These benefits are then reflected in the cost of operations. Reduced production costs for the DISA translate to reduced prices for the customer, thereby enabling the Department to more effectively accomplish its mission within available resources.

The DISA capital budget includes IT equipment and software assets (including security investments) used by the DISA to provide communication and computing services. In addition, the DISA will provide equipment such as workstations on a lease basis. Funding for the development, manufacture, or procurement of IT capital assets for a DBOF customer of the DISA will be provided by the customer, and will be reflected in the customer's capital budget. If an IT asset is procured by the DISA in support of one or more DBOF business areas, it shall be capitalized on a pro rata basis in the financial records of each business area and depreciated over the approved life cycle of the item.